Social Media: Some Things to Consider Before Creating an Online Presence

CPT Adam Jonasz, JAG, USA

Introduction

One-way communication between military commands and their Soldiers, Family members, civilian employees, and the public is going the way of the VHS, the floppy disk, and the dinosaur. Command policies, safety briefs, training calendars, and traditional ways of conveying orders at daily formations, on bulletin boards, or through word of mouth is taking a back seat to more modern methods and mediums of communication. Soldiers, Family members, employees, and the public no longer just listen, and commands and commanders no longer just speak and expect to be heard; they now engage in a conversation. This conversation is not always a physical face-to-face exchange, but an increasingly virtual one over the internet through the use of "social media" forums like Facebook, Twitter, YouTube, and Flickr.

What is said on the parade ground is now posted on Facebook. What Soldiers and/or units do during training, in the field, or in the combat zone is now broadcast on YouTube. What Soldiers discussed at the chow hall or in the barracks now appears on Twitter. Comments are now memorialized on the internet, through posts, video, or audio, and all of it available to millions of users with the simple click of a mouse. Social media can be about engaging in conversation, changing the conversation, directing the conversation, listening to the conversation, responding to the conversation, starting the conversation, or just getting the word out.

Historically, commanders at all levels were able to determine the parameters of the relationship they had with their Soldiers and the Soldiers had with them. Now, because of the prevalence of social media and the Army's increasing use and reliance on it, Soldiers, Families, Army civilian employees, and the public are the ones who increasingly define how the unit or commander is perceived and the direction and course of their relationship.

Purpose

This article is an overview of social media and some of the many benefits, concerns, and legal issues to consider when deciding whether or not to create and maintain a government external official presence (EOP) within the social media world. In addition, it is the intent of this article to provide commanders, units, and organizations within the Army Medical Command (MEDCOM) tips on how to successfully ensure editorial control of your EOP. This article was not written with the intent of being an analysis of MEDCOM social media sites or as an in-depth report on the legal authority, laws, and guidance covering the use of social media. For guidance or details on how to set up a social media site, see *The Army Social Media Handbook 2011*[1] which contains guidance, many tips, and contact information to assist organizations with the implementation and maintenance of a social media page.

Overview

In order to fully grasp the idea of social media, it may help to parse the words. Media is the plural form of the word "medium," which in this context is a means of communication, such as radio, newspaper, the internet, or television that reach and influence people widely. Social media is therefore a social means of communication, in a 2-way environment as opposed to a one-way format. In the context of the internet: a website that does not simply present information, but allows for interaction while presenting information. This interaction can be as simple as asking for feedback or letting you vote on an issue, or it can be as complex as target advertising based on websites you previously visited or things purchased in the past.

Social media is a very broad term and, depending upon with whom you are speaking and for what purpose they engage in or use social media platforms, you may get a variety of definitions. For our purposes, however, social media usually refers to a large range of websites that allow online communications in which individuals shift fluidly and flexibly between the roles of audience and author. Social media can also be defined as the content created and shared by individuals on the web using freely available websites that allow users to create and post their images, video, and text information, and then share that with either the entire internet or just a select group, depending on security or privacy settings.

The Army's Use of Social Media

The Army has long recognized the extensive use of the internet and especially social media websites by society at large, but specifically Soldiers, Family members, potential recruits, and Army civilian employees. The Army presence in the social internet environment began in 2007 and has been increasing rapidly ever since, with EOPs being sponsored/maintained by general officers and commanders at all levels, including organizations down to platoon-size elements.[2]

The Army quickly recognized the importance of the fact that social media provides users the capability to rapidly and efficiently communicate with large numbers of people over a 2-way communications platform using multiple media such as audio, video, photo, and text. By using existing software platforms or websites such as Twitter, Flickr, YouTube, and Facebook, the Army can connect and interact with Soldiers, Families, Army civilians, and the public with little or no monetary investment. Most importantly, the Army is attempting to make use of social media platforms to affirmatively communicate the Army message to the public, Soldiers, Families, Army civilians, and people all over the world. The Army is taking control of the message, creating the conversation and listening to what is being said. As of October 2010, there were 1,076 registered EOP sites as follows: Facebook 713, Flickr 130, Twitter 162, and 71 on YouTube.[2(p3)]

On February 25, 2010, Department of Defense (DoD) Directive-Type Memorandum (DTM) 09-026[3] established DoD policy and assigned responsibilities for responsible and effective use of internet-based capabilities, including social networking services. The DTM also provided basic guidelines for military use of social media, and the use of an EOP. The policy went further by clearly stating:

> This policy recognizes that Internet-based capabilities are integral to operations across the Department of Defense.[3(p1)]

The DTM defined internet-based capabilities as:

> All publicly accessible information capabilities and applications available across the internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet based capabilities include collaborative tools such as SNS, social media, user generated content, social software, e-mail, instant messaging, and discussion forums (eg, YouTube, Facebook, MySpace, Twitter, Google Apps).[3(p1)]

It also defined external official presence as:

> Official public affairs activities conducted on non-DoD sites on the internet (eg, Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter.)[3(p1)]

In addition, the Memorandum presented DoD policy as follows[3(p2)]:

> The NIPERNET* shall be configured to provide access to Internet-based capabilities across all DoD Components.
>
> Commanders at all levels and heads of DoD Components will continue to defend against malicious activity affecting DoD networks (eg, distributed denial of service attacks intrusions) and take immediate commensurate actions, as required to safeguard missions (eg, temporarily limiting access to the internet to preserve operations security or to address bandwidth constraints.
>
> Commanders at all levels and heads of DoD Components will continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites (eg, pornography, gambling, hate-crime related activities).
>
> All use of internet-based capabilities shall comply with paragraph 2-301 of Chapter 2 of the Joint Ethics regulation…and the guidelines set forth in Attachment 2 [to the DTM].

On March 25, 2010, the Chief Information Officer of the Army issued a memorandum[4] which addressed establishing, maintaining, and reviewing social media sites, as well as operations security (OPSEC) awareness and training requirements.

On October 21, 2010, the Secretary of the Army issued a memorandum[5] establishing the delegation of authority for EOPs to the commanders of all Army commands, who may then redelegate the authority to subordinate commands, direct supporting units, and field operating agencies.

On March 1, 2011, the Deputy Secretary of Defense reauthorized Attachment 3 (Responsibilities) of DTM 09-026,[3] extending the DTM through January 2012 and outlining how the NIPERNET should be configured to allow access to Internet-based capabilities throughout the DoD components.

DoD and Department of the Army Regulatory and Policy Guidance on Social Media

At this point there are several regulations and directives that currently direct the Army's use of social media. According to the *Army Social Media Handbook 2011*,[1] the

*Nonsecure internet protocol router network

Assistant Secretary of Defense is currently working on an all-encompassing policy. Until that policy is issued, guidance is found in DTM 09-026[3]; a June 17, 2009 memorandum from the Office of the General Counsel of the Army[7] which recommended training for creators and maintainers of websites, content review for OPSEC, and other prohibited information and use disclaimers; and the following publications:

- *Army Regulation 25-1.*[6] Along with the Chief Information Officer (CIO)/G-6, the Chief of Public Affairs oversees and controls content on Army public websites. Only official Army information that is releasable and of value to the public may be released on these sites. Commanders and organization heads are to ensure that the Public Affairs Office and other appropriate designees review and clear web content and format before the content is posted on the Internet. The primary responsibility of the CIO/G6 is managing the Army's network, to include providing the appropriate amount of bandwidth to allow access to internet-based capabilities across the Army networks per DoD policy.

- *DA Pamphlet 25-1-1.*[8] Each Army organization that establishes a public website must have a clearly defined purpose and website plan that supports the organization's mission. All individuals appointed as webmasters or site maintainers, reviewers, and content managers must complete training and certification, as necessary, appropriate to the duties assigned to them.

- *Army Regulation 530-1.*[9] The regulation provides guidance to all Army Soldiers, civilians, and contractors to eliminate, reduce, or conceal indicators that could result in releasing critical and sensitive information. The regulation addresses the review requirements for releasing Army or government information through all types of media.

- *Army Regulation 360-1.*[10] Any official information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to DoD must be cleared by appropriate security review and public affairs offices before release. This includes materials placed on the internet or released via similar electronic media. The Office of Public Affairs has the authority to release information about the Army as a whole; commanders below Headquarters, Department of the Army level can release information wholly within the mission and scope of their respective commands.

The Office of the Chief of Public Affairs (OCPA) has produced 3 documents to assist commands and organizations with their social media programs. On February 12, 2010, it released a Social Media Best Practices (Tactics, Techniques and Procedures) slideshow that outlined basic guidelines for public affairs social media strategies. On November 1, 2010, OCPA issued a memorandum titled "Standardizing Official US Army External Official Presences,"[11] in an attempt to standardize Army-wide EOPs. The OCPA published *The Army Social Media Handbook*[1] in January 2011, followed by a revised, updated version in August 2011.

As OCPA is also responsible for maintaining the Army social media registry, it apparently has taken the lead on developing policy and monitoring how social media is used in the Army. OCPA has also taken center stage in the effort to educate commanders and agencies on the use of social media and its potential pitfalls.

To establish a social media site, units/commanders must, at a minimum, consult the Secretary of the Army Memorandum: "Delegation of Authority – Approval of External Official Presences,"[12] and Attachment 2 (Guidelines For Use Of Internet-Based Capabilities) to DTM 09-026.[3] Units/organizations must receive command approval before establishing an EOP and it must be approved by the release authority (commanding officer or public affairs) before it can be registered (an EOP must be registered). When submitted for approval and registration an EOP plan must contain the following: a point of contact with a valid military (.mil) email address, a URL to an official Army website, a posted disclaimer which identifies the page as an "official" Army social media presence and disclaims any endorsement. The site must be clearly identified as official, unlocked and open to the public, use official seals, logos, be monitored and evaluated by DoD components for compliance with security requirements, and ensure info posted is accurate and relevant and does not provide personally identifiable information or information not approved for release. It is recommended that anyone considering establishing an EOP consult their public affairs office for advice and guidance. Public affairs plays a prominent role in the Army's use of social media and are constantly updating and implementing new ways to assist in the execution of Army regulations and DoD guidance.

LEGAL OVERVIEW

An overview of the legal principles that cover government sponsored social media include but are not limited to the following: the 1st Amendment to the US Constitution, copyright laws, the The Privacy Act of 1974,[13] the

Federal Open Records Act (Federal Records Act of 1950, 44 USC §§29,31,33), and defamation. Federal agency public web pages are required to comply with the provisions of section 508 of the Rehabilitation Act Amendments of 1998 (29 USC §794d). Public web pages must be equally accessible to disabled and nondisabled federal employees and members of the public. These legal issues should not inhibit or deter any organization from using social media to advance the unit mission, however, decision makers should be aware that social media does not exist in a vacuum. As a forum of media, many of the laws that apply to newspapers, television, radio, and magazines also apply to social media. Furthermore, when governmental agencies take part in social media, laws that relate to government action apply as well.

When a government actor creates a web presence, which is a forum for communication, it involves the 1st Amendment right to freedom of speech and expression. Therefore, the first issue to address is whether or not that agency's web page created a "public forum." A public forum is a US constitutional law term that describes a government-owned property that is open to public expression and assembly.[14] There are several types of public forums, each one expanding the right of public expression.

The most open forum is the traditional public forum, such as streets or parks that, by long tradition, have been devoted to the public for expressive use. In the traditional public forum, the government may not impose content-based restrictions on speech unless they are "necessary to achieve a compelling state interest and…narrowly drawn to achieve that end."[14] A social media page is unlikely to be designated a traditional public forum, as the US Supreme Court has restricted that category to property "historically" used for public expression (eg, public square in front of a court house or a municipal park).[14] Currently, social media space or the internet do not fall within that description. However, with time that may change as constitutional interpretation evolves.

The designated public forum, which "consists of property which the state has opened for use by the public as a place for expressive activity."[14] Examples include a public university "campus free speech zone" open to all speakers, or meeting rooms in a public library which is available to all members of the public. A designated public forum requires the government's clear intent to open one, however, it could be inferred based on the government's policies and practice. What the Supreme Court has termed the limited forum could be considered a subcategory of the designated public forum. The limited public forum is a place or space designated for speech by "certain groups" or for "discussion of certain topics." The government's establishment and application of content parameters in the limited public forum must be "reasonable in light of the purposes of the forum," and viewpoint neutral.[14]

The nonpublic forum refers to government property that "is not by tradition or designation a forum for public communication."[14] In a nonpublic forum, deference will be given to the government actor in deciding who may speak and what shall be said. The government may impose time, place, and manner restrictions, and may exclude speakers as long as that exclusion is reasonable.[14]

The last category is government speech. The concept behind this category is that governments must speak in order to govern, and they do so through agents whom they hire, pay, recruit, or subsidize. The government is permitted to use media to communicate its message and, when it does so, it does not have to include opposing viewpoints or allow for an exchange of idea or any interaction.[14] The ballot box is where the public has the opportunity to respond.

The type of public forum becomes important when deciding issues concerning whether defamatory or vulgar material would be protected by the 1st Amendment, what comments can be removed, what information may be retained or collected, and what information may be tracked. A question for commanders in regards to a social media platform is whether a commander or site maintainer can remove profanity or hate speech from a page? For example, can he or she order the removal of a post by someone who asks a controversial question, or makes a divisive or contentious remark?

The type of public forum created may very well determine the amount of editorial control and whether a post is actually a public record, and, if so, whether or not there is an obligation to maintain, release, and/or distribute. The type of social media presence maintained by the organization may be determined in part by the contents of any user agreement and its terms and conditions, disclaimers, and the stated purpose/scope of the site. Most government actors, including military organizations, create solely informational social media pages (eg, using Facebook without any interaction) and are engaging in purely government speech, and therefore retain editorial control of the page. The problems that usually arise concern EOPs that operate between the 2 extremes of no interactivity and complete interactivity. This gray area of having some interaction between web page creators and visitors to the site, but yet strictly controlling the conversation, scope of interaction, and/

or content makes it much more difficult to determine whether or not the government sponsored social media page is a public forum.[14]

Most of the time, the deciding factors will be the site's purpose, content, user policies, disclaimers, and the quantity and/or quality of communication between visitor and site creators/maintainers. At this point, there is no need for a constitutional law discussion about whether or not a particular EOP created a public forum. For purposes of this article, it is sufficient for the reader to be aware that, by their very nature, government-sponsored EOPs or web pages, regardless of purpose or content, fall under a constitutional umbrella which may or may not affect the extent to which a government actor, by its power to control the conversation, may utilize and control the capabilities of a social media site.

Retaining Editorial Control

If a government actor is very careful in setting up its social media site, it can usually guarantee that it is either government speech or a nonpublic forum and can therefore retain maximum control over the conversation that takes place. Lidsky[14] suggests the following combination of actions and common sense solutions for government agencies and commanders to ensure that their organization's site falls into a public forum that allows them to retain as much control as possible over the content and conversation:

- Establish a direction or purpose, a real objective that serves to advance your mission. The purpose may evolve as long as you develop a strategic plan to support it. Clearly state and post the purpose and the scope of site on the first page so that it is noticeable to visitors to the site. It should state that the use of social media by (name of entity) is for the purpose of obtaining or conveying information that is useful to or will further the goals of said entity.

- Plainly describe the terms and conditions of use so that a visitor to the site and/or user is on notice as to what kind of conduct and content is prohibited or permitted. Remind Soldiers that their conduct on the site is still regulated by the Uniform Code of Military Justice[15] and that they are expected to conduct themselves accordingly. Review the current applicable guidance and request advice from the public affairs office to ensure you are covering all of the Army specific requirements.

- Identify an administrator/maintainer in charge of the site. The maintainer should be well trained on all policies regarding EOPs, OPSEC regulations and concerns, and on reviewing content before it is posted. He/she should be intimately aware of the objective of the site. Require them to use their names and titles for official posts or responses.

- Establish a policy for the retention of records. This very simply means that anything posted by the organization or comments by the public should be retained in some form that, if needed, can be retrieved at a later date.

- Make sure that the administrators/maintainers understand the technology, how a site works, how to post, and how to remove posts. They must be knowledgeable about the subject matter, comprehend the commander's or unit's intent, and be able to apply that understanding responsibly to the web page. The administrators/maintainers must know the law, regulations, and guidelines before creating the site, as well as during its operation. Contact your local public affairs office, staff judge advocate and security officer for information and assistance.

- State clearly what kind of forum that you are creating. This could be done implicitly in the purpose/scope/policy statement. However, stating your intent to create a nonpublic or limited public forum immediately informs the visitor and user that there is no absolute 1st Amendment right to free speech or expression on the site.

- Train your people well and give them the time and resources to accomplish your site's stated purpose.

- Clearly post your disclaimers. They should include a general disclaimer, privacy and security disclaimer, copyright and trade mark disclaimer, moderated presence disclaimer, persistent cookie disclaimer, Freedom of Information Act (5 USC §552) and records management notice, external links and nonendorsement disclaimer, and all disclaimer/notices required by Army regulations. Include a disclaimer that states that any content posted by the public, Family member, Army civilian employee, and Soldier does not represent the opinion of the command.

- Clearly state user policies, terms and conditions, and enforcement methods such as no use of profanity; no personal attacks; no spam messages; no off-topic comments; no solicitations; failure to follow guidelines for posting comments may result in the deletion of comments without warning; and, based

on the discretion of site officials, comments may be deleted if they violate the Uniform Code of Military Justice,[15] disrupt good order and discipline, are discriminatory or offensive.

- Keep postings in official capacity. Do not speak/post/comment in an unofficial capacity, nor fluctuate between the 2 capacities.

One crucial indicator of the type of public forum your organization creates is the amount of interactivity that the site permits. Make an unambiguous resolution as to whether comments from the public, Soldiers, and/or Family members will be allowed. If allowed, develop standards that will limit topics, organizational subjects, or issues to those first posted by the command. As the strategic plan and/or the purpose of the site is under development, commands should determine how they will respond to posts and how much they will engage in conversation with the users.

The command must decide how to respond, or even whether to respond to questions or comments that are posted on the site. It must be determined how to manage unwanted or controversial comments or questions, or to leave them on the site either answered or unanswered. On some sites, other users may police such comments by either answering them (correctly or incorrectly) or by expressing disapproval of such comments or approval. Site administrators must decide at what point to remove divisive posts or to officially comment on them. The approach that a command adopts may change during the life of the site, depending upon the organization and the site's purpose/objective, negative or positive feedback from users, and/or the particular message or conversation.

Benefits And Challenges To Using Social Media

Before engaging in the use of social media, commanders and agencies in MEDCOM must first ask themselves whether the benefit received will warrant the time, expense, and effort involved in the creation and maintenance of an EOP on a social networking website.[14] They must seriously evaluate all the benefits and potential drawbacks or difficulties associated with having a presence on a social media website. Most importantly, before anything else, commanders and organizations must determine for what "purpose" they are undertaking this enterprise, ie, for what reason is a social media presence required? Commanders and organizations should not create social media web pages simply because other agencies are doing it, it is a modern form of media, or because it looks good on a résumé.

Once the purpose or objective has been determined, a strategic plan or social media strategy is necessary to establish how the purpose or objective will be achieved. A well organized and structured social media plan must address the following questions:

- What direct benefit does it offer the organization, agency, unit or command?
- What are the potential dangers, pitfalls or drawbacks?
- What are the legalities involved in operating a social media page?

In addition, commands should be knowledgeable about the process, requirements, and basic guidelines that govern the establishment, use, and maintenance of an EOP.

There are ample reasons why a commander, an organization, or even a platoon-size unit would want to use social media to enhance the mission. Social media is a powerful communication tool that can significantly increase the effectiveness of a command's interactions with Soldiers, Family members, civilian employees, and the public. Social media provides the command with the ability to reach larger audiences, including people with whom the command would not otherwise interact during the ordinary course of business. This communication can take place on a consistent basis, faster, and less expensively than with other forms of media. The quality of the communication is enhanced as well, through the use of video, audio, computer generated images, and photos. Today people can view social media anywhere at any time through desk tops, laptops, Ipads, Ipods, cell phones, at work, home, in the car, or while shopping. It can be used very effectively in crisis situations, to provide warnings and information, and manage a response. It can help build and maintain morale and esprit de corps by keeping the command and Soldiers connected.

Interactive social media can serve as a virtual town hall meeting, encouraging interaction between the command and its constituents. Social media also encourages the exchange of information and collaboration between the command and Soldiers, Families, and civilian employees, providing a continuous process of consultation. The command determines its amount of engagement. Social media can be used exclusively as an information outlet, or it can be used to solicit open-ended comment and expression, or to request more focused and limited avenues of feedback. The command can use it as a tool to encourage an exchange of ideas, to address relevant issues or concerns, monitor attitudes about certain issues,

and get a sense of the overall temperament across the target audience.

Commands can use social media sites to communicate with Soldiers, Families, and employees, directly eliminating intermediaries. Posts from the commander or command sergeant major are communicated directly and give an aura of straightforwardness without distortion. Social media fosters a spirit of engagement, accessibility, approachability, and the atmosphere of responsiveness between the command and its constituents.

Perhaps the greatest advantage of social media is that it allows the command to control the message. The message is whatever the command determines will promote or advance its mission. The message the command communicates is designed, tailored, and managed by the command. The command determines the message content, when, where, and how it is released, and the target audience. It may be as simple as posting information about organizational events, administrative necessities, or to congratulate a Soldier on a special occasion. The message can be directed at certain groups, individuals, or organizations; it could be to correct a wrongly perceived event or inaccurate news story. The message may be influenced by the kind of feedback the command receives from the message it posts. However, the means to track and measure feedback and the manner in which feedback is delivered are also controlled by the site administrators.

Not only can the command or organization dictate the message, it can control and/or limit the amount of interaction. In actuality the command shapes and manages the tone, quality, nature, and direction of the conversation that takes place by simply controlling the topic or subject of discussion; limiting the time allowed for comment; restricting the type of comments received (positive, constructive—not negative or divisive); establishing whether any comment is allowed; if allowed, the form of the comment (text, video, or a simple vote type response), and its length. The type of message and reply/comment environment may reflect the type of relationship the command has with its Soldiers, Family members, Army employees, and the public.

Drawbacks of Social Media Use in the Military

Although there are great benefits to using social media and it can be a force multiplier when used appropriately, in the context of government, especially the military, social media use comes at a price. Interactive social media can create or exert pressure to respond to user demands, comments, or questions. Site controllers must be careful what they ask for, or to what extent they open the conversation. Users and visitors are allowed their opinions. Obviously, Soldiers, Family members, Army civilians, and the public have 1st Amendment rights to free expression. The candid, uncensored exchange of ideas, and the freedom to express complaints, ask questions, and/or make comments is what has defined social media. However, that very characteristic is a potential game changer for military commands and organizations because the necessity to control the conversation is key. Even though the conversation occurs on an impersonal illuminated screen, there is still the requirement to maintain and convey the message of a command-driven relationship, with good order and discipline.

Many commands, organizations, and individual commanders choose not to respond to user comments or posts, but observe and listen. Even when comments or suggestions are requested, or questions are asked, those commands and/or individual commanders do not respond. Depending on an organization's strategic communications plan and social media purpose, such an approach can present a constant dilemma . Many users or visitors to a site will judge the site's credibility on the amount of interaction and conversation that occurs: how responsive is the site, is it consistently responding or not at all, is it merely an informational site, or does it support an actual exchange of ideas. Each command, organization, and/or commander must decide to what extent and when they will engage with a user based on upon their overall strategic plan. However, a site's perceived relevance to and prominence among its intended audience may depend upon how they view the site's credibility.

The most obvious and dangerous concern surrounding the use of social media in the government and specifically the military is the loss of sensitive or classified information. The internet is a powerful way to convey information quickly and efficiently. However, it also provides a potent instrument to adversaries to obtain, correlate, and evaluate an unprecedented volume of aggregate information regarding our operational capabilities, security limitations, and vulnerabilities. This spillage of information into the public arena can be used to assemble fragments of information to decipher the larger picture, draw conclusions, and deduct usable and actionable intelligence.

Maintaining operations security and the ability to manage the risks that result from the use of social media should be the number one priority of site controllers/maintainers. Information in the wrong hands can compromise ongoing operations, base security, or result in identity theft. Operations security includes information

concerning things such as: force protection measures; communications (information management, infrastructure information systems and networks equipment); logistics (movement of equipment and troops); personally identifiable information of Soldiers and Family members; operations (training missions, tactical and strategic operational military actions) and critical infrastructure (eg, bases, nuclear facilities, water plants).[9] Operations security concerns exist in what may seem like harmless photos, videos, news announcements, or status updates—not just folders clearly marked SECRET.

Operations security considerations should be part of any strategic social media plan. Site organizers must be aware of and knowledgeable about Army regulations that apply to classified and sensitive information, and who can approve the release of information. Operations security awareness training and specialized training for site maintainers and controllers is a must and should be included in the budget when determining the costs of establishing a site. Furthermore, site administrators/maintainers should be intimately familiar with the intent or purpose of the organization's social media page. Sometimes, unclassified information that might be considered harmless may not be conducive to the command's social media plan and should not be posted. The commander is ultimately responsible for the content of the organization's social media pages, including the problems that occur: a security violation, an offensive comment by a site official, or a simple mistake about the time and date of a social event.

Beyond the potentially dangerous reality of the release of OPSEC-related material via a social media site, site operators must be concerned with the dissemination of misinformation or a misrepresentation that may be posted by impostors or impersonators. In addition, site operators/maintainers must be trained on how and when to enforce site policies, user agreements, and disclaimers. For example, a site maintainer should be well trained regarding what posts or comments can be censored or deleted from the site, and when and if they need to be recorded and maintained.

Depending on the size of the organization and site's purpose, maintaining a social media presence can be a very time-consuming, labor-intensive endeavor. Social media page site operators must be trained not just on OPSEC issues, but in technical operation and maintenance, compliance with Army regulations and command policies, and site policies. The operators must design, create, manage, and promote the site. They must consistently review the site's content; keep the site interesting, people engaged, and information updated. The list of responsibilities goes on and on, and everything must be accounted for in the strategic plan, then resourced and funded.

Because the commander is personally responsible for the content, operation and maintenance of the site, he/she should be involved in or at least informed about its daily operations. Once a site operator publishes a post/comment, it becomes the commander's responsiblity. Once that comment, photo, or video is in the public domain, control over that post is basically lost; it can be downloaded, copied, and distributed at will. The command must also monitor the tone of its comments/posts (friendly but professional), review the photos, video, or text before publication. The sponsoring command must make every effort to not violate its own policies, protect copyright and trademark laws, and monitor and track feedback. If the purpose of the site is to connect with an audience with which the command does not interact on a regular basis, a poorly maintained or unremarkable site without much (or any) site/user interaction will not have many followers. It will lack credibility. A poorly organized and maintained site becomes irrelevant and may give a visitor/user a negative impression of the command and organization.

There are additional factors that an Army MEDCOM organization commander should consider when using or deciding whether or not to use social media are. The potential risk of an unauthorized release of personally identifiable information (PII) associated with patients' medical records/histories, civilian medical personnel, insurance providers, credentialing, investigations, lawsuits, and Family members is enormous.[16] Protection of personal information under the Privacy Act[13] and the Health Insurance Portability and Accountability Act (Pub L No. 104-191 (1996)) is an essential and basic responsibility of all MEDCOM organizations working with or connected to the provision of healthcare. It is usually these very kinds of organizations that could benefit the most from an open, uninhibited exchange with its users. However, the more open and engaging the site may be, the greater the potential risk for an unintended release of information. Unauthorized releases or a loss of PII is an extremely serious event, commands and site operators should refer to *OTSG/MEDCOM Policy Memorandum 11-070*[16] for reporting incidents when there is a suspected or actual loss, theft, or compromise of PII.

Records management is another factor that must be considered by organizations that provide healthcare. Records include all books, documents, videos, photos; indeed, anything made or received by the agency as evidence of the organization, function, policies, practices,

procedures, policies, operations, or other activities; or because of the informational data they may contain. The Federal records Act of 1950 contains the statutory authority for the Army Records Information Management System. Any electronic information generated by or contained in an information system or other automation source that is created or received during the conduct of business must be preserved. There are also restrictions on the collection of information from members of the public and how that information is stored. According to the Paperwork Reduction Act of 1995 (44 USC 3501 et seq), government agencies must get approval from the Office of Management and Budget prior to obtaining or soliciting "identical" information from 10 or more persons. The information must then be stored incompliance with the Privacy Act.[13]

The very nature of the medical field involves the use of copyright, trademark, and patent materials; equipment; instruments; and pharmaceuticals.[17] Site operators must be ever vigilant not to endorse, promote or show support for one product over the other. They must be mindful not to wrongfully use record, distribute or portray copyrighted material, patents or trademarks without acquiring the prior consent of the proprietor. For example photographs from media reporters working with units ("embedded") are copyrighted and cannot be publicly distributed without the written consent of the reporters.[17]

Conclusion

Like many other Army commands, MEDCOM organizations have turned to social media to distribute their message. In the MEDCOM there are numerous traditional websites and social media sites that span the spectrum of interactivity and communications. Because of their unique mission, many Warrior Transition Unit (WTU) sites have demonstrated a willingness to engage in conversation. Rather than waiting to be overwhelmed by questions and/or complaints from Soldiers, Family members, and/or interested third parties and see the reputation of the command suffer, some WTUs took a more proactive approach to establishing a communications platform for the command. Although social media has worked well for WTUs, that does not mean it will work, or is even a viable communications option, for all MEDCOM organizations.

Because of the nature of the Army's overall mission; the traditional, customary and legal restraints that surround open discourse within the military; and the necessary structure of the command/subordinate relationship, oftentimes the most advantageous social media site is one with restricted interactivity, offering informational and administrative necessities, while still providing a limited avenue of access to the command. Not all commands can afford to open themselves to full and free communication exchanges with users, for such openness of expression may negatively affect the way the command delivers its message, interacts with its subordinates, or even alter or inhibit the actual, intended purpose of the site.

Army MEDCOM organizations that already have an EOP in operation and those considering creating one should recognize and appreciate certain basic realities. The more an organization opens the site for a back and forth exchange of comments/posts, the more it is unable to control the conversation and messages of the forum. Consequently, it then becomes harder to manage the risks associated with OPSEC and PII. There is a greater obligation to maintain and keep records, protect 1st Amendment rights, and train and keep qualified personnel to monitor and maintain the social media platforms.

Finally, unfortunately, a simple fact that is often overlooked by too many organizations when sponsoring a social media page is that the command must determine how to keep the EOP relevant and prominent with users. Commands must consistently engage, participate (to a limited extent), influence, and monitor. The crucial element to a successful governmental or military social media site is "credibility." If users think a commander, command, or organizational site is credible, they will keep coming back—they will connect with it. The site will be relevant and take a prominent place in the user's choice of communications media within the command. A reliable site will attach an appearance of credibility to the command and/or organization. That perception alone has the potential to advance the mission.

The reader should recognize that all organizations do not require a social media site, nor is it to their advantage. Is it really necessary that we receive a tweet from a commander about what they had for breakfast or that a Soldier can become a fan of the command on Facebook? We certainly can read newsworthy articles on the organizational web page, in the newspaper, or in the base or organizational paper. Commanders can still get the message out at formations, bulletin boards, through town hall meeting, email, written correspondence, by phone, or face to face.

Commanders must consider how their organization's page will impact the larger picture, how it fits in with the overall Army message, and, most importantly, is a social media page really going to advance their units mission. Bottom line: considering all the legal implications,

benefits, and risks is creating an EOP really worth it, or can you simply do it the old fashioned way?

References

1. *The United States Army Social Media Handbook Version 2*. Washington, DC: Office of the Chief of Public affairs, US Dept of the Army; August 2011. Available at: http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011.
2. *The Army's Use of Social Media External Official Presence Sites*; Alexandria, VA; US Army Audit Agency; July 26, 2011. Audit Report; A-2011-0150-IET.
3. *Directive Type Memorandum (DTM) 09-026: Responsible use of Internet-based Capabilities.* Washington, DC: Deputy Secretary of Defense; February 25, 2011: Change 2. Available at: http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf.
4. Chief Information Officer/G-6 Memorandum: Responsible Use of Internet Capabilities. Washington, DC: Office of the Secretary of the Army; March 25, 2010. Available at: http://ciog6.army.mil/LinkClick.aspx?fileticket=Es8pnrXtvdU%3D&tabid=64.
5. Memorandum: Delegation of Authority–Approval of External Official Presences. Washington, DC: Secretary of the Army; October 21, 2010. Available at:http://www.slideshare.net/USArmySocialMedia/delegation-of-authority-social-media-use.
6. *Army Regulation 25-1: Army Knowledge Management and Information Technology.* Washington, DC: US Dept of the Army; December 4, 2008.
7. Office of the General Counsel Memorandum: Use of Social Media in the Army. Washington, DC: Dept of the Army; June 17, 2009.
8. *Department of the Army Pamphlet 25-1-1: Information Technology Support and Services.* Washington, DC: US Dept of the Army; October 25, 2006.
9. *Army Regulation 530-1: Operation Security.* Washington, DC: US Dept of the Army; April 19, 2007.
10. *Army Regulation 360-1: The Army Public Affairs Program*. Washington, DC: US Dept of the Army; May 25, 2011.
11. Department of the Army Memorandum: Standardizing official U.S. Army external official presences (social media). Washington, DC: Office of the Chief of Public Affairs, US Dept of the Army; November 1, 2010. Available at: http://corpslakes.usace.army.mil/socialmedia/Social%20Media%20Standard%20SOP.pdf.
12. Secretary of the Army Memorandum: Delegation of Authority–Approval of External Official Presences. Washington, DC: US Dept of the Army; October 21, 2010. Available at: http://www.slideshare.net/USArmySocialMedia/delegation-of-authority-social-media-use.
13. USC §552a (1974).
14. Lidsky LB. Government sponsored social media and public forum doctrine under the first amendment: perils and pitfalls. *The Public Lawyer.* 2011;19(2).
15. 64 Stat. 109, 10 USC, chap 47.
16. OTSG MEDCOM Policy Memorandum 11-070: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures. Fort Sam Houston, TX: US Army Medical Command; August 19, 2011.
17. *Army Regulation 27-60: Intellectual Property,* Washington, DC: US Dept of the Army; June 1, 1993.

Author

CPT Jonasz is an Attorney-Advisor with the Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.